# Virtual Private Cloud-as-a-Service: Extend Enterprise Security Policies to Public Clouds

# Virtual Private Cloud-as-a-Service: Extend Enterprise Security Policies to Public Clouds

White Paper

## What You Will Learn

Public sector organizations without the budget to build a private cloud can consider public cloud services. The drawback until now has been tenants' limited ability to implement their own network security policies.

This white paper, intended for public sector IT personnel and public cloud service providers, describes a new public cloud architecture that enables tenants to preserve their existing enterprise security policies:

- Today, Virtual Private Cloud (VPC) customers who want to implement their enterprise security policies need to pay for dedicated physical networking infrastructure, significantly increasing costs.
- Now cloud providers can offer a virtual switch as a service, giving tenants the same security capabilities without the high costs of a dedicated switch.
- Public cloud providers who use the Cisco Nexus® 1000V Switch can offer VPC as a service (VPCaaS) as well as other network security services, enabling customers to extend their enterprise security policies into public clouds.

# Virtual Private Cloud-as-a-Service: Extend Enterprise Security Policies to Public Clouds

## The Case for Public Clouds in the Public Sector

Governments and educational institutions are beginning to use cloud services for infrastructure as a service (IaaS), software as a service (SaaS), and platform as a service (PaaS). The primary motivation is to lower costs by sharing infrastructure such as servers, storage, and switches.

One of the first decisions is whether to build a private cloud or use a public cloud service. For public sector organizations that have the budget, private clouds are the best option because the IT team maintains complete control over security and service levels.

But if the capital budget or management resources for a private cloud are not available, public clouds are an attractive option. Instead of paying up front to build the private cloud infrastructure, you pay a usage-based fee to the cloud provider for compute resources, memory, storage, VLANs, firewall, load balancing, and so on.

### Security Challenges of Public Clouds

Public sector organizations initially hesitated to use public clouds because of security concerns associated with shared infrastructure. These objections are diminishing with the introduction of Federal Information Security Management Act (FISMA) certifications for public cloud services. Beginning in June 2012, public cloud providers will also be able to earn Federal Risk and Authorization Management Program (FedRAMP) certifications. FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Other ways that public cloud tenants can mitigate application security risks include keeping the operating system up to date, activating OS security features, and enabling security features such as SSH and SSL.

Achieving enterprise-class network security in public clouds has proved a tougher challenge. The barrier is that multiple tenants share the same physical switches, preventing individual tenants from applying their own network security policies. This is problematic because an organization's security policies are tightly integrated with the network.

For example, consider a government agency that maintains three connections to each server: one each for client access, one for connecting to the backend database, and one for storage replication. The enterprise policy might stipulate protections for each of the three networks, including dynamic host configuration protocol (DHCP) snooping and VLAN access control lists (ACLs); stateful firewalling among the interfaces; and intrusion prevention. The policy might also call for limiting access to Windows XP clients with a specified patch level. Most of today's public clouds do not support these options because tenants cannot access the physical switch infrastructure.

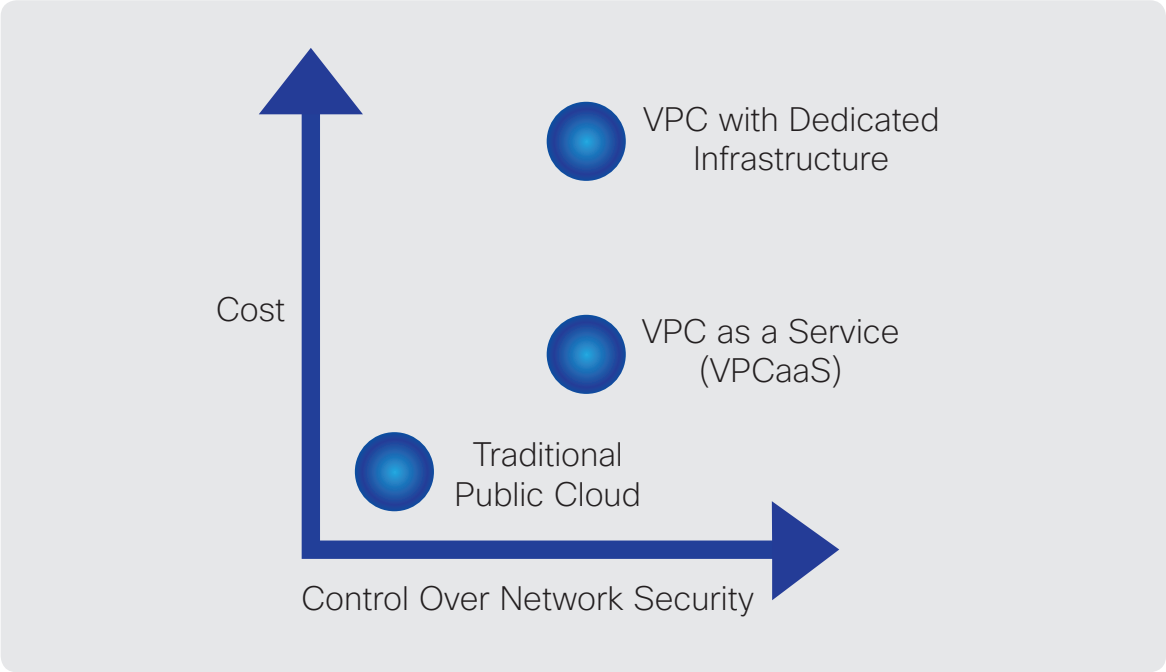
Realizing the importance of networking security to their public sector customers, major public cloud providers now offer VPC services. Customers typically receive multiple VLANs with network address translation (NAT) and a VPN connection to the customer's own data center. However, tenants cannot configure the shared switch to provide security protections. Therefore, government customers who need this control must pay for dedicated networking infrastructure, negating the cost savings that drew them to the public cloud in the first place.

## Middle Ground: Virtual Private Cloud as a Service

With the advent of virtual switches, public cloud providers can now offer VPC as a service (VPCaaS), giving public sector customers full control over network security policies without the high costs of dedicated infrastructure. When cloud service providers offer VPCaaS, the public cloud becomes an extension of the customer's enterprise network.

Figure 1 compares the degree of control over network security to costs for standard public cloud offerings, VPCs, and VPCaaS.

**Figure 1 VPC as a Service Provides Flexible Security Control Without High Costs of Dedicated Infrastructure**



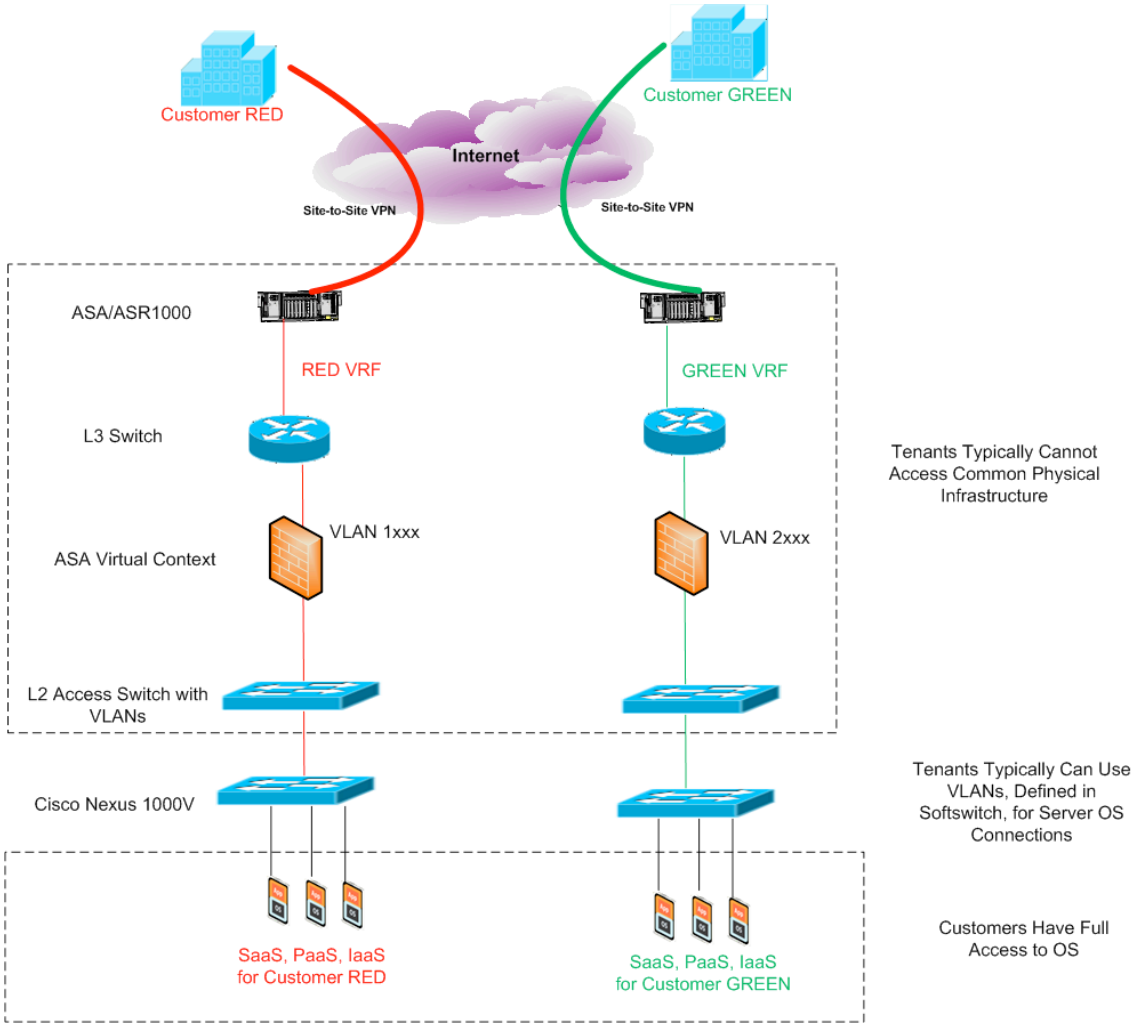
# Virtual Private Cloud-as-a-Service: Extend Enterprise Security Policies to Public Clouds

## How the Public Cloud Provider's Infrastructure Affects Network Security

Unlike organizations without stringent security requirements, public sector organizations need and benefit from understanding the cloud provider's architecture, especially as it applies to security capabilities.

Figure 2 illustrates a typical multitenant public cloud. The service provider logically separates each tenant's traffic using IPsec VPNs, Virtual Route Forwarding (VRF), VLANs, and firewall security contexts. However, only the service provider can access the shared network infrastructure shown at the top of the diagram. As stated earlier, tenants have no access to these physical switches and can enforce their security policies only if they pay for dedicated switch hardware.

Figure 2 Cisco Reference Architecture for Virtualized Multitenancy Data Center



Tenants using the architecture shown in Figure 2 can, however, directly access virtualized OS-level services shown at the bottom of the diagram, including SaaS, PaaS, and IaaS. These services are accessed through virtual switches that support multiple virtual environments using virtual access control lists (VACLs) and private VLANs.

What if cloud providers offered the virtual switch as a service, just as they currently offer other infrastructure as a service? In this model, each cloud tenant receives dedicated virtual switch services, gaining full control to extend existing enterprise security policies into the public cloud.

## What You Can Do with a Virtual Switch

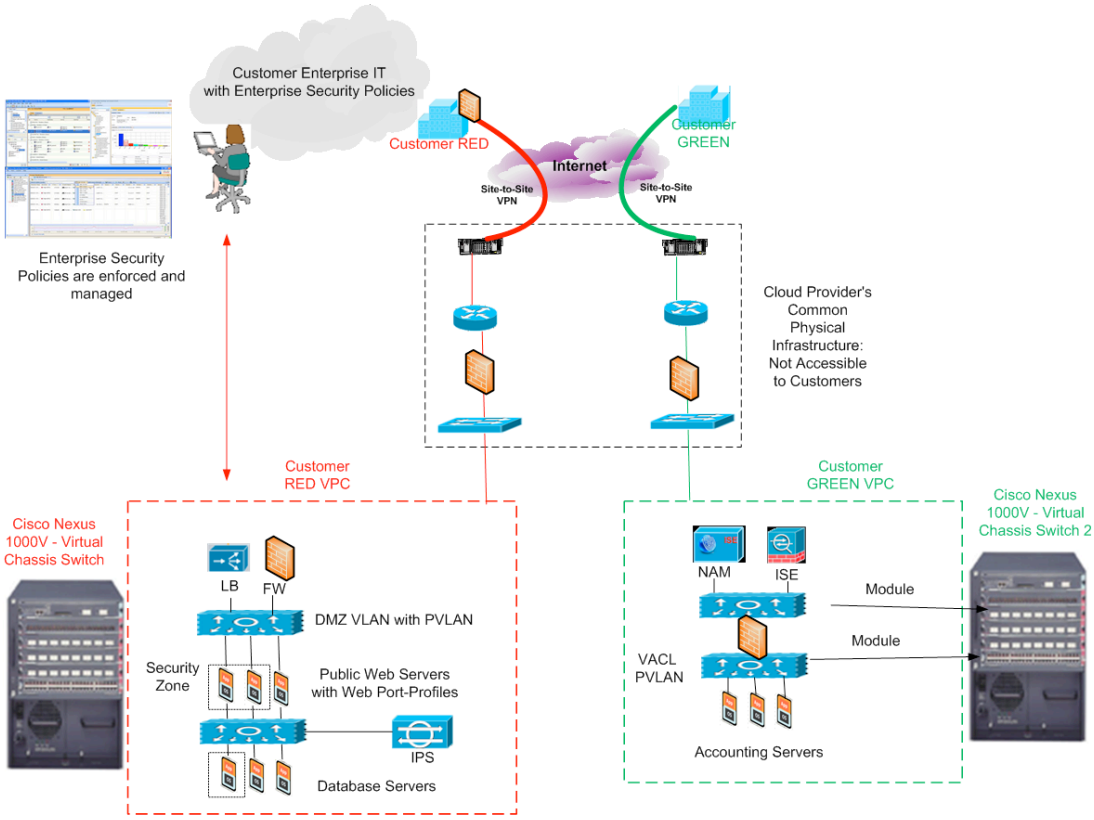
Not all virtual switches are the same, however. Most, for example, do not provide visibility into virtual networks. The Cisco Nexus 1000V Switch gives cloud customers the same level of security that they would experience with a dedicated physical switch, including:

- Network visibility: Public cloud tenants acquire the same degree of network visibility they would have with a dedicated physical switch, including seeing which virtual servers are connected to the switch.
- Traffic monitoring: Tenants can use Cisco IOS® NetFlow technology to monitor traffic for billing, planning, and security.
- Defining security settings for each switch port: Using Cisco Nexus 1000V port profiles, tenants can define security settings for each switch port. If you already use port profiles in your own data center, you can use the same profiles in the cloud. If not, you can create new port profiles based on your physical server security settings and apply them to your virtual machines. Port profiles follow virtual machines as they move between physical servers in the cloud, as when the cloud provider uses VMware vMotion to move VMs to different blade servers during busy periods or for server maintenance.
- Enforcing security policies based on MAC addresses: This is useful in virtualized environments, where MAC addresses are dynamic rather than burned in.
- Access to additional security services: Cloud providers that deploy the Cisco Nexus 1000V Switch can also use it as a platform to offer security services from Cisco and other vendors. Cisco® security services include Virtual Security Gateway (VSG), virtual wide-area application services (WAAS), and a virtual network analysis module that inspects packet content. Cisco is also adding a virtual Adaptive Security Appliance (ASA) to support stateful filtering for virtual machines and enable tenants to connect directly to their zone using IPSec.

# Virtual Private Cloud-as-a-Service: Extend Enterprise Security Policies to Public Clouds

Figure 3 illustrates a VPC that gives each public cloud customer full control of the customer's own virtual switching environment.

Figure 3 Extending Enterprise Security to the Public Cloud



# Virtual Private Cloud-as-a-Service: Extend Enterprise Security Policies to Public Clouds

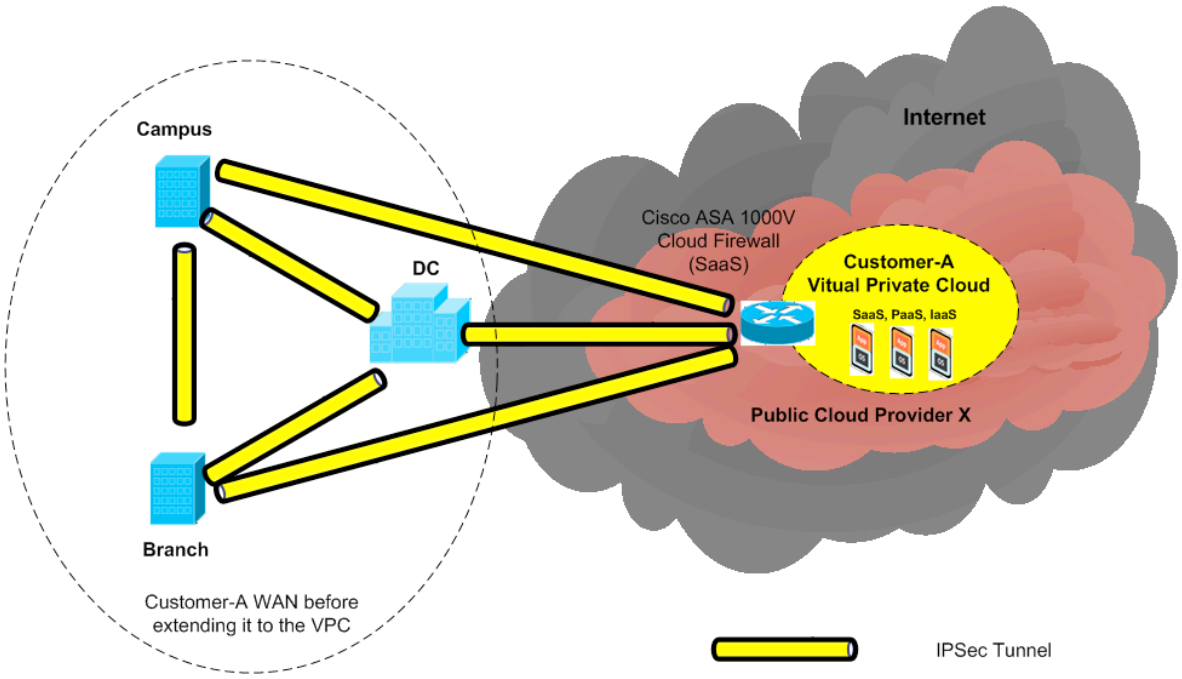
## Next Steps: Virtual Private Cloud as Extension to the Enterprise Network

Private cloud customers gain even more control when providers offer customers the option to define WAN security policies that make the VPC look like a branch office or another data center. This is different from popular IPsec-based VPNs already available from public cloud providers. With an IPsec VPN service, customers cannot control the physical firewall devices that enforce IPsec policies because the devices are part of the common infrastructure.

The solution is a new type of SaaS: the Cisco ASA 1000V Cloud Firewall. This firewall operates as a virtual machine that customers can configure and fully control to enforce their own security policies. The customer's policy information is not visible to the public cloud provider (see Figure 4).

Another public cloud model on the horizon is for customers to provide their own equipment for deployment in the cloud provider's data center, and manage the equipment themselves. This is the reverse of today's model, where service providers deploy their own customer premises equipment (CPE) at customer locations and manage it remotely. The new model meets the needs of federal agencies that are required to deploy hardened routers and special encryption devices.

Figure 4 VPC as Extension of Enterprise Network



## Conclusion

While private clouds remain the best option for public sector organizations, public cloud innovations such as VPCaaS and routers as a service are narrowing the security gap between private and public clouds. By selecting a public cloud that uses the Cisco Nexus 1000V Switch, public sector customers position themselves to take advantage of these security services when available. The vision is to extend enterprise security policies into the public cloud, making the VPC an extension of the enterprise network.

Government organizations can accelerate the continued evolution of public clouds by sharing their requirements with cloud providers.

### For More Information

To learn more about the Cisco Nexus 1000V Switch, visit: www.cisco.com/go/1000v.

To read Cisco Nexus 1000V technical documentation, visit: www.cisco.com/go/1000vdocs.

To participate in the Cisco Nexus 1000V community, visit: www.cisco.com/go/1000vcommunity.

To learn more about the Cisco ASA1000V Cloud Firewall, visit: www.cisco.com/en/US/products/ps12233/index.html.